Remarks

Claims 1 is herein amended and new claims 2-20 are added thus leaving claims 1 – 20 pending in this application. Upon entry of this amendment, which is earnestly solicited, the applicant respectfully requests favorable examination on the merits of all pending claims.

A marked-up copy of claim 1 clearing illustrating only the amendment thereto is provided herewith for the Examiner's convenience. In addition, a clean copy of all pending claims is provided for examination on the merits.

Should the Examiner wish to discuss the instant patent application or this Preliminary Amendment, the applicant hereby invites telephonic or electronic contact at the number and e-mail address provided below.

Respectfully submitted,

Dated: December 28, 2001

Paul H. McDowall, Reg. No. 34,873
LARKIN, HOFFMAN, DALY & LINDGREN, LTD.
1500 Wells Fargo Plaza
7900 Xerxes Avenue South
Bloomington, Minnesota 55431
pmcdowall@lhdl.com (e-mail)
(952) 896-3220 (direct)
(952) 896-3333 (fax)

717328.2

In the Claims
(Marked-Up Version Showing Changes)

1. (Amended) A method for recognizing and refusing [DoS] denial of service and [DDoS] distributed denial of service attacks on server systems of network providers and operators by means of an electronic intermediary device implemented in a computer network, wherein the electronic intermediary device contains a computer program for carrying out defense for a target computer system against the [DoS] denial of service and [DDoS] distributed denial of service attacks, for each one of a[n IP] network connection request, performing the following steps:

registering the [IP] network connection request and storing a data packet associated with the network connection request in a computer memory;

checking the validity of the registered [IP] network connection request and the data packet associated with the network connection request, and while the [registered] data packet is being checked for validity;

sending a periodic acknowledgement signal to preserve the network connection between the target system and the network connection request, and after receiving confirmation of the validity of the [IP] network connection request;

forwarding [a] the data packet associated with the [IP] network connection request to [a] the target system which was the subject of the [IP] network connection request.